POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Title:	SPMP Integrated Risk Assurance Universe	**Meeting Date:**	21st May 2024
Author:	Anshu Mathur, Group Assurance Director	**Sponsor:**	Sarah Gray, Interim Group General Counsel

Input Sought: Approval

The Committee is asked to:

- **Approve** the additions made to the SPMP Integrated Risk Assurance Universe.
- **Note** the status of the SPMP Assurance Reviews.
- **Approve** the 34 Statement of Works.

1. SPMP Integrated Risk Assurance Universe – For Approval

In the period since the last ARC in March 2024, we have made the following changes to the SPMP Integrated Risk Assurance Universe:

- **Governance Pillar**
  Based on feedback from the GE SPMP Sub Committee in March 2024, we have now added 4 P1 risk lines/items to capture Business Case (BC) and Benefit Realisation (BR) Assurance. As a consequence the Governance pillar has 21 risks vs 17 previously.

  Whilst the Assurance teams (both SPMP and Group) currently do not have the capability to deliver BC and BR assurance, funding has been secured to recruit.

The SPMP Integrated Risk Assurance Universe therefore comprises 509 (previously 505) inherent risk spread across 16 pillars. Please refer to **Appendix 1** for the current snapshot of the SPMP Integrated Risk Assurance Universe.

2. Statement of Works (SoW) - Approval

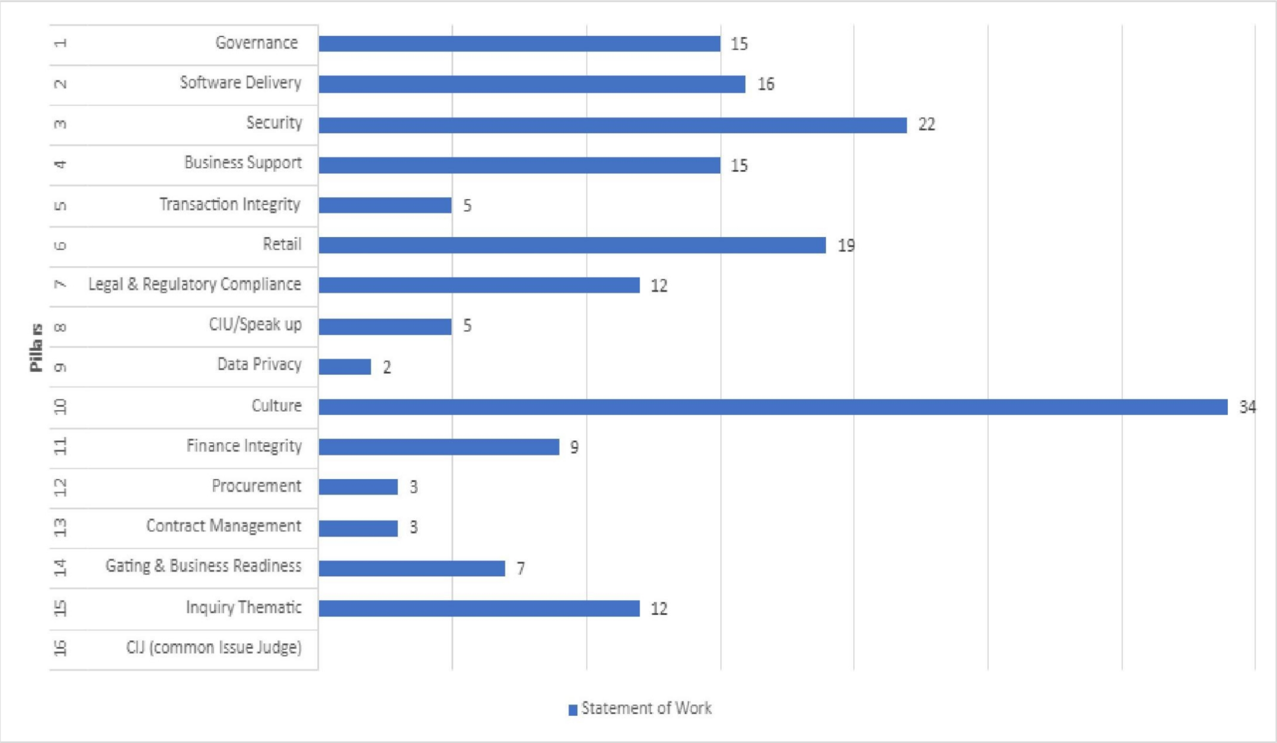
As mentioned in the ARC in March 2024, we have now completed drafting 34 SoW defining the assurance scope and coverage of risk lines. As shared with ARC, we have applied the following principles to determine the coverage and scoping of SoW:

- Adequate coverage of material key risks (P1's, where appropriate P2's and P3's).
- End to End assurance to provide a programme and business view of readiness.
- Assurance coverage across pillars to ensure efficiency and eliminate rework, if possible.
- Clear assessment of Postmaster protection and or KRI's.
- Adequacy of design (where applicable – effectiveness) of Controls.
- Identify SoWs that may need periodical refresh, contingent on release strategy.
- Coverage and mapping of HIJ and CIJ.

By applying the above principles, we have ensured adequate coverage exists not only from a pillar perspective but also from an inherent risk lens:

- **Pillar coverage** - The table below demonstrates that the 34 SoWs touch all 16 pillars:

Coverage of SoW per Pillar



A few key things to note are:

- CIJ spans across Transaction Integrity, Finance, Security, Retail, Business Support, Data Privacy, Software Delivery.
- Transaction Integrity spans across: Finance, Data, Security, Business Support, & Retail.
- Culture will be a core underpin of all our reviews.

- **Inherent Risk coverage** - The 34 SoWs provide 100% coverage of all the P1. Please refer to **Appendix 2** which shows the coverage of inherent risk per SoW.

Appendix 3 provides the details of SoW scope and the assurance outcomes. Please note, these SoWs form the initial premise from which assurance work will commenced and are considered draft and not exhaustive, as input will be taken from Business / Programme / SMEs / Stakeholders (internal and external) before finalising the Terms of Reference.

We have not provided anticipated timelines for when these 34 SoW would be delivered, as this is very much contingent on resourcing, capability, allocation of external assurance support, risk profiles of SPMP releases, and the completion of the first 5 SoW.

3. SPMP Assurance Tracker

The table below provides the status update for the 5 SOWs as at 15 May 2024:

	SOW	SOW Ref	Terms of Reference	Fieldwork	Planned Reporting	Planned Completion
1	Business Requirements	SOW 1	April 24	April 24	June 24	June 24
2	Defects and Risk Management	SOW 6	April 24	April 24	June 24	June 24
3	Security / User Access – Account management, access control, audit logging and user access	SOW 5 & 8	April 24	April 24	June 24	July 24
4	Transaction Integrity	SOW 3	May 24	May 24	June 24	July 24
5	Retail Readiness (NEW)	SOW 26	April 24	May 24	June 24	July 24

Legend: Completed On Track Delayed

Whilst progress has been made, we have not in full earnest commenced fieldwork. This is primarily driven by the Assurance Team(s) focus on ensuring all SoW are drafted. In addition, the drafting and finalisation of Terms of Reference were more complex than initially thought and required wider business engagement.

Group Assurance are engaging with the programme to assess whether we continue to have the right composition and capability to deliver the assurance programme. The programme has recently approved to hiring of two assurance resources to support delivery of the assurance programme.

For SoW 5 and 8 (Security / User Access – Account management, access control, audit logging and user access) the SPMP assurance team are engaging with a 3rd party service provider TMC3 who have been brought into look at data breaches by the SPMP Programme management team. The provider at present is planning to conduct a root cause analysis of the 2 breaches identified and the Statement of Work for this Phase is being drafted by TMC3. The functional assurance team will ensure that there are no duplications of assurance through understanding TMC3 scope before executing any detailed work.

We have also, subject to ARC retrospective approval, are planning to commence SoW 26 to focus on Retail Readiness to receive the SPMP platform (both pilot and waves). The ToR for this review will be shared and discussed with the Retail Engagement Director to ensure key operational insights are captured from a legacy perspective.

4. Other Updates

- **Procurement - External Assurance SME Support**

  After the initial pre-market engagement held from February to March - the initial engagement engaged with 10 suppliers, of which 5 remain (PA Consulting, Ernest & Young, Crowe Consulting, Protiviti and Credera).

  A sourcing strategy has been created (informed by market engagement) has been submitted to PDB, Steerco, SEG in May and Board for approval to proceed in June 2024.

  The preferred procurement option would be to release a single FTS procurement but as this would take 4-6 months to complete the plan is to split procurement activity into two phases.

- **Phase 1** Review the current SPMP Integrated Assurance & Risk Universe for completeness and against industry best practice.
- **Phase 2** Create the invitation to tender (ITT) with a detailed set of requirements derived from the universe and a plan for assurance that can be provided to the market, including commercial protections for both the bidder and POL on 'how' assurance outcomes will be presented.

Group Assurance are also working in parallel to create a contingency worst-case scenario where POL may have to create their own internal pool of SME Contractors.

- **Recent external review on SPMP:**

For the committees awareness two external reviews have been performed on SPMP, which management are in the process responding to and preparing remedial actions plan.

In our opinion, both reports highlight consistent concerns on the deliverability of SPMP. Key extract from these reports are summarised below:

- **Infrastructure and Projects Authority (IPA) Draft Report**

For the Committee's awareness, in April 2024 IPA performed a review on Horizon Replacement (SPMP, SDES, and Horizon Extension), this covered gates 0 to 3 to support a Treasury Approval point of the Programme Business Case for funding between June 2024 and March 2026. Their scope covered:

- Gate 0 – Looks historically on the delivery of the Horizon replacement programme
- Gate 3 – Test the maturity and robustness of the Programme Business Case
- The review also assesses whether governance arrangements across interested and invested oversight and delivery partners remains effective and robust.

IPA 's draft opinion is as follows: '**RED** - Successful delivery of the 3 POL Programmes that deliver the Horizon replacement to time, cost (defined in the business case under consideration) and quality appears to be unachievable. There are major issues which, at this stage, do not appear to be manageable or resolvable entirely within POL. The programme/project may need re-baselining and/or its overall viability re-assessed.'

According to their rating guidance – 'This programme/project should not proceed to the next phase until these major issues are managed to an acceptable level of risk and the viability of the project/programme has been re-confirmed.'

The review identified three strategic issues that could help sustain these high-risk programmes through to successful conclusion:

(1) Providing clarity of governance, now Horizon replacement is on Government Major Projects Portfolio (GMPP). There is confusion about which of the 3 programmes are coming onto GMPP and this needs to be resolved.
(2) We are recommending government consider if the financial arrangements are appropriate for these programmes.
(3) It is the right time for a meaningful conversation about risk appetite as only a common understanding of this across all governance bodies involved, will enable the programme, and especially the technical development of NBIT, to be successful.

The review recognised that Programme Leadership has been tackling poor quality and weak management controls (especially planning, monitoring, and reporting and proper risk based assurance) and improving quality of technical development. The report has identified 7 recommendations that management are in the process of working through.

- **Public Digital (PD) Report – Final**

  On behalf of DBT, PD have completed a review of SPMP and New Branch IT. The goal of the review was to assess the viability of SPMP in meeting POL's future needs, focussing on POL's capability to deliver the programme, the technical approach being taken, value for money and other factors. Their key observations are summarised below:

  - Whilst trending in a generally positive direction with pocket of excellent work and deeply expert people, SPMP overall is not currently in a healthy place.
  - There are significant gaps in strategy, capability, technology and Governance that need addressing.
  - A high level of management churn along with lack of corporate memory, presents a risk of the past (lessons from previous failed attempt to re-platform) repeating itself.
  - Throwing ever more resources at the problem will not solve the problem.
  - SMPM's viability is being undermined by serious deficiencies in its governance, technical, and implementation approach.
  - The responsibility and accountability to fix the issues does not sit only with the Programme. It will require the whole of POL, and key partners in UKGI and DBT to work together to do this.

  Key findings:

  - The vision and dominant framing of SPMP does not align with an overall POL strategy, is not agreed and understood by the wider POL business, and is not consistently recognised within the SPMP programme
  - The organisation lacks permanent people with critical capabilities and experience, and there is an absence of continuity in keystone functions, particularly in leadership and management, which creates unacceptable risk to the programme.
  - Historical technology choices and development practices, adopted to attempt to meet significantly different past programme goals, have left significant technical debt in the heart of the product. Good practice and standards have now been codified, but are not yet in place across the full delivery organisation.
    - Weighing pros and cons, we concluded that if our review team was leading the project despite the obvious sunk costs we would give very strong consideration to reintroducing an off-the-shelf ePOS solution as the core retail element, while retaining all the integration work that the teams have invested time in.
  - POL's recent history is driving a fear of accountability for decisions, resulting in risk aversion and a governance model unsuited to the need. The programme, business, and wider stakeholder ecosystem must work as "one team" towards shared outcomes
  - The programme is not truly user-centred and the professional practice of "product management" is not well understood inside POL. This has resulted in an inconsistent approach to product development that has become disconnected from delivering value to users.

5. Key Next Steps

1. Focus on commencing and completion of the 5 SoWs in flight.

POL00460600

2. Assess adequacy / capability of Assurance resources – June /July 2024.
3. Commence G-Cloud 13 engagement to commence work on Phase 1 of the work required to support assurance - May 2024.
4. Obtain approval from the PDB, Steerco, SEG for the 2 Phased procurement approach - May 24, followed by Board approval at the June 2024 meeting.
5. SPMP functional assurance and Group Assurance to work on a paper to create a plan B for an internal pool of SME Contractors - June 2024.

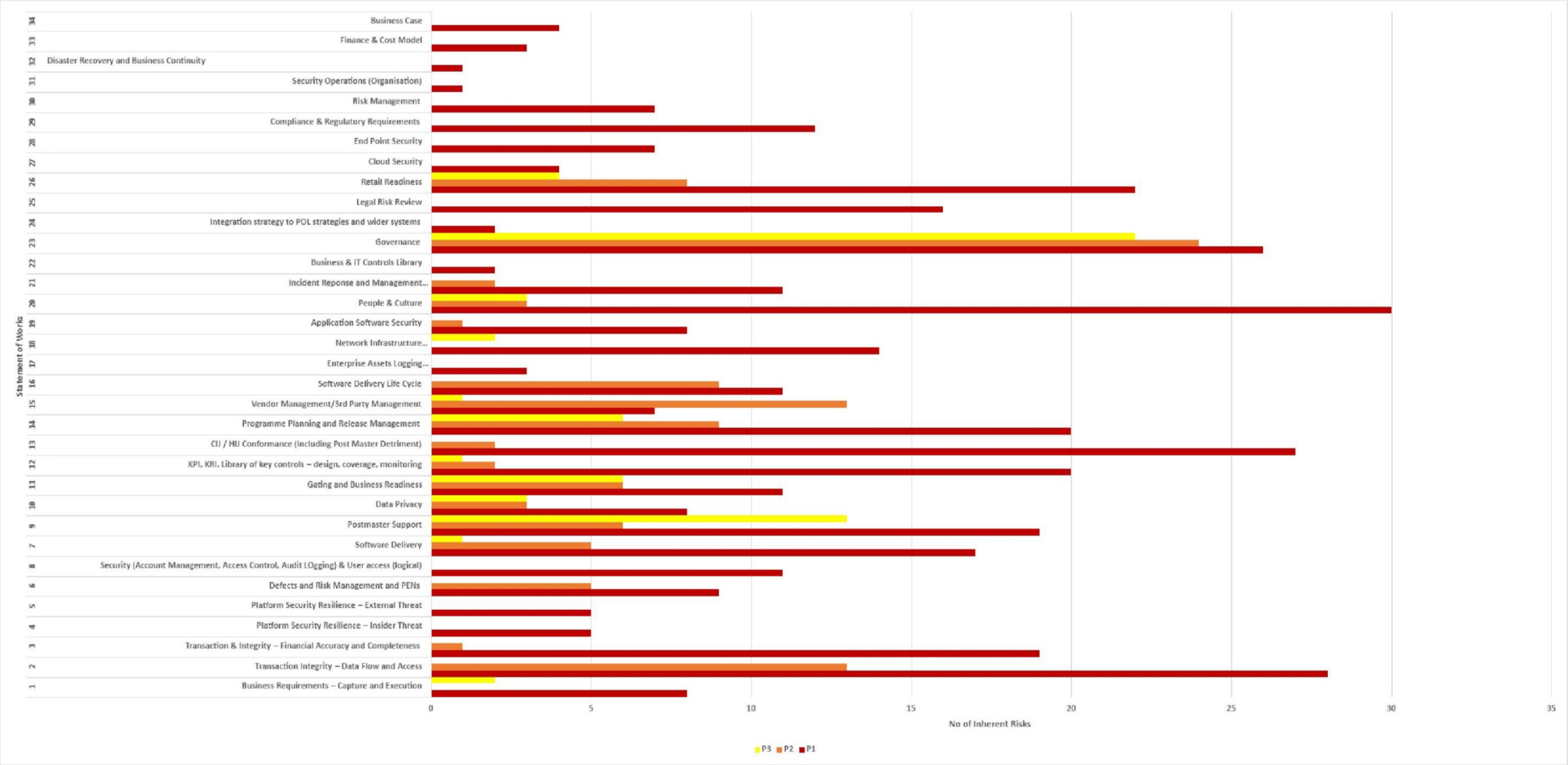
POL00460600

Appendix-1- SPMP Integrated Risk Assurance Universe – 30 April 2024

No	Pillars	Inherent Risks	P1	P2	P3
1	Governance	26 (22)	*21 (17)	2	3
2	Software Delivery	29	24	4	1
3	Security	24	24	0	0
4	Business Support	81	20	39	22
5	Transaction Integrity	19	7	12	0
6	Retail	48	22	22	4
7	Legal & Regulatory Compliance	27	13	6	8
8	CIU/Speak up	57	57	0	0
9	Data Privacy	23	20	3	0
10	Culture	14	11	3	0
11	Finance Integrity	26	26	0	0
12	Procurement	8	0	8	0
13	Contract Management	8	1	7	0
14	Gating & Business Readiness	10	0	1	9
15	Inquiry Thematic	67	67	0	0
16	CIJ (common Issue Judge)	42	19	14	9
	Total	**509**	**332**	**121**	**56**

*Note: Change in the period is highlighted in yellow (prior figure).

Appendix 2 - So~~O~~W Coverage of Inherent Risks



Appendix 3 –SoW's – [These will continue to be evolved and updated with business and SME input.]

SOW #	Title	Key Pillars	Scope	Assurance outcome
1	Business Requirements – Capture and Execution	1. Governance 2. Business Support 3. Data	To ensure the programme has implemented a structured methodology for the ownership, capture, execution and change management of Business Requirements. This will be an End-to-End review with a focus on: 1) Compliance with all legal, regulatory, operational, commercial requirements and how featured in the Business Requirements (including HIJ / CIJ considerations). 2) Alignment with the Business Case. 3) Ensure effective translation of the requirements covering Data and Security into the Business Requirements. 4) Document management to support status and amendments throughout the programme delivery cycle. 5) Construct of testing (e.g.UAT) to ensure essential elements of the requirements are proven against deliverables. 6) Effectiveness of governance and oversight. 7) Clearly defined process, controls, reporting and organisation structure (+RACI) to support all the above.	Programme can demonstrate a clear audit trail of requirements, and their lifecycle, including implemented vs not, and oversight. Clear evidence / artefacts provided to support how Business: 1) Requirements were initially captured and maintained /controlled throughout the programme delivery cycles. Including change controls process. 2)Proof that all essential elements of the programme deliverables (e.g. regulatory / data / CIJ /Security, TI etc) have been defined and appropriately sign off. 3) All testing (e.g. UAT) has been aligned with Business Requirements to ensure compliance as necessary. 4) Processes / controls in place, and followed, and aligned with best practice.
2	Transaction Integrity – Data Flow and Access	1.Transaction Integrity 2.Business Support 3.Retail 4.Security	To ensure key data flows are mapped and documented. And to ensure that access to relevant data sets is defined by roles and transactions. Obtain and review the Architectural design and set up of the new platform and the data flow diagrams which sits alongside. Understand ownership and change management protocols. Review the Integration linkages to other systems to ensure these have been identified and defined with dependencies/risks. Understand the Integration plan and testing strategy, including the stage gate sign-offs. Review roles designs and set ups and how these relate to the transaction objects and related information access through these objects.	SPMP has a defined data flows and data set. And that rule sets and roles exist to manage the access and visibility, including security. Clear Architectural design diagrams with supporting data flow diagrams. With clear ownership and accountabilities for the different data sets. Integration linkages clearly documented with risks and dependencies. With relevant supporting integration plans. Clear role designs and responsibilities with supporting access management to data and transactions.

SOW #	Title	Key Pillars	Scope	Assurance outcome
3	Transaction & Integrity – Financial Accuracy and Completeness	1. Finance 2. Retail 3. Legal & Compliance 4. Business Support	To ensure the financial accuracy / completeness of transactions and relevant controls and monitoring is in place. Review the reports that are planned or available to support financial transactions including reports that support the sub-ledgers and general ledger and production of financial statements-cash flows, Income Statement, Balance Sheet etc. Review and assess design of exception reports designed to support daily, weekly, month, quarterly and annual operations. Assess whether controls and reconciliations (Control Framework) built into the process to ensure relevant Management Review Controls can operate successfully.	SPMP ensures Financial Transactions are complete, accurate, supported and evidenced. With reporting and monitoring in place to identify and correct any identified issues, exception, anomalies etc.
4	Platform Security Resilience – Insider Threat	All pillars, key focus on 1. Security 2. Finance 3. Retail 4. Business Support 5. Inquiry	To ensure the platform can withstand insider threats - To validate that robust controls are in place to protect the platform from unauthorised access and DLP (Data Loss Prevention). Supported with the relevant training and awareness. Assess whether tooling is in place to identify (proactively and retrospectively), capture and report on insider threats and assess whether remediation processes are set in place to counter such instances. Review adequacy of MI and EWI in place to support the business processes reporting and management, including oversight/reporting at a senior level. Including a review of the following: • Continuous vulnerability Management • Audit Logging Management • Malware defences • Data Recovery • Penetration Testing • IT/DR Recovery. And identifying and understanding Policies, Procedures and training in place at POL and CISO input.	SPMP is accessing and designing preventative and monitoring measures to manage Insider threats. Control's must be fully documented and supported by KPI/KRIs. Supported with the relevant MI that is timely and accurate for management to take relevant actions to prevent or detect future threats.

SOW #	Title	Key Pillars	Scope	Assurance outcome
5	Platform Security Resilience – External Threat	All pillars, key focus on 1. Security 2. Finance 3. Retail 4. Business Support	To ensure the Network Infrastructure can withstand external threats. Adequate preventive and monitoring mechanisms are designed: • Assessment of network architecture, configuration, & security controls. • Evaluation of firewall configurations, intrusion detection/prevention systems, and network segmentation. • Review of network devices, such as routers, switches, and access points, for vulnerabilities and misconfigurations. Including a review of the following: • Continuous vulnerability Management • Audit Logging Management • Malware defences • Data Recovery • Penetration Testing • IT/DR Recovery. And identifying and understanding Policies, Procedures and training in place at POL and CISO input.	SPMP is accessing and designing preventative and monitoring measures to manage External cyber threats. Control's must be fully documented and supported by KPI/KRIs. Supported with the relevant MI that is timely and accurate for management to take relevant actions to prevent or detect future threats.
6	Defects and Risk Management	All pillars, key focus on 1. Software Delivery 2. Hyper Care 3. Business Support 4. Transaction Integrity 5. Security 6. Governance 7. Retail	To assess application and documentation of testing/defect methodologies across the end-to-end software delivery life cycle. To ensure appropriate ERM is applied in the assessment of defects (functionality, performance, Security, etc) and or acceptance of defects vs risk profiles in isolation and or in aggregate. Assess appropriate sign off and governance applied to testing and defects management. To ensure PEN's are managed, prioritised and addressed in accordance with good business practice and reviewed and approved with those in authority.	SPMP has applied testing in a consistent manner, with appropriate consideration to risks and key SME are involved in risk assessments and decision making. Clear evidence that defect management and PENs are well managed with robust controls, measures and align with good business practice, with the relevant approvals and oversight.
7	Software Delivery	All pillars, key focus on 1. Software Delivery 2. Hyper Care 3. Business Support 4. Transaction Integrity 5. Security 6. Governance 7. Retail	Review of software delivery processes / development life cycles processes and procedures. Assess application of good practices, process methods, testing eg UAT, defect management and compliance with the defined deliverables. Assure whether all activities clearly controlled and documented. Overlap - Controls around defect management will also feature as part of this review.	Clearly able to demonstrate throughout the Software delivery stages that good practice has been applied and supporting documentation / artefacts available to support decisions, conclusions and approaches adopted.

SOW #	Title	Key Pillars	Scope	Assurance outcome
8	Security (Account Management, User Access Control, Audit Logging) & User access (logical))	1. Software Delivery 2.Security 3.Retail 4.Business Support 5. Hyper Care 6. Transaction Integrity	To assess that adequate preventive and monitoring controls are designed over Access and Identity Management. To assess whether super users' profiles are commensurate with roles/profiles. Review whether all profiles accessing data (read only, edit, etc) are identified and controlled. Including a review of the following: • Review of IAM (Identity and Access Management) processes, including user account provisioning process, authentication, and access controls, Access control lists • Assessment of privileged access management (PAM) controls. • Evaluation of single sign-on (SSO) and multi-factor authentication (MFA) implementations. • Analysis of Access logs and audit trails • Automated tools or scripts used for scanning and assessing access configurations. And identifying and understand Policies, Procedures and training in place at POL and CISO input.	To assess whether the programme understands the technology landscape to pinpoint exhaustively points of access (PM. POL. Third parties, etc). SPMP user access is structured, defined, exhaustive and governed. And authentication is robust from a security perspective, including the Segregation of Duties (SoD).
9	Postmaster Support	1.Retail 2.Transaction Integrity 3. Business Support 4. Culture 5. Gating 6. Business Readiness	To assess whether processes and procedure, designed and documented to support PM transition to SPMP. Assess efficacy of PM Training/communication etc. Review whether issue judgments have been appropriately considered and actioned – HIJ, CIJ, Training. Assess whether hyper care is designed around PM.	Training and Detailed Procedures are in place to support Post master's both pre and post go-live. Hypercare arrangements and Business Support processes and procedures are fit for purpose to support PM in transition. Robust governess supported by adequate and appropriate EWI, KPI's and KRI's.
10	Data Privacy	1. Data 2. Security 3. Transaction Integrity	To review and assess whether Data Privacy principals are appropriately designed and embedded to protect Postmaster, POL, and other key sensitive data types. Assess adequacy of: • Data classification, encryption, and access controls. • Assessment of data retention policies and procedures. • Compliance with data protection regulations (e.g., GDPR, HIPAA, CCPA).	SPMP has designed and deployed Data Privacy principles that protect PM and POL, And other sensitive data. Appropriate and relevant restrictions and encryption are in place to support security and protection of data and ensure compliance to relevant data protection regulations.
11	Gating and Business Readiness	1. Governance 2. Business Support 3.Software Delivery 4. Retail, Security 5. Legal & Compliance 6. Gating	Assess whether Gating decisions are based on sound data and MI, and key SMEs input. Review the E2E gating process / methodology to ensure appropriate controls are in place to provide key decision and control points in the programme's delivery life cycle.	SPMP has a clear methodology and approach for gating and business readiness. With the relevant governance to ensure that key SMEs are involved in decision making and outcomes documented to evidence the decision-making process.

POL00460600

SOW #	Title	Key Pillars	Scope	Assurance outcome
12	Library of key controls – design, coverage, monitoring including efficacy of KRI, KPI, EWI etc.	1. Governance 2. CIJ 3. Security 4. Business Support 5. Transaction Integrity 6. Retail, 7. Data 8. Finance 9. A&CI	To review whether the design of key indicators/controls to ensure POL has adequate coverage on the E2E platform and sufficient early warnings designed to ensure no adverse impacts to PM or POL. Assess whether appropriate RACI and DOA (Delegation of Authority) in place to ensure timely visibility and decision making. Review whether a library of controls, with clear ownership, accountability and tracking exists.	POL governance is designed appropriately with adequate MI and escalation by design, to support and ensure an appropriate control environment.
13	CIJ / HIJ Conformance (Including Postmaster Detriment)	All pillars will be engaged throughout all reviews with a specific focus at point of "go live"	To assess that lessons from the past have neem embedded in SPMP design and clear outcomes and that mistakes and errors will not be repeated. This will involve a line-by-line review to access how issues from the past (CIJ & HIJ) have been or are being address by the programme and BAU Assurance.	SPMP can clearly demonstrate lessons have been learnt and all HIJ / CIJ observations have been addressed as part of design, build, test, and deployment. And that clear monitoring mechanics are in place contingent of the release strategy of SPMP.
14	Programme Planning and Release Management	1. Governance 2. Business Support 3. Software Delivery 4. Finance 5. Gating & Business Readiness 6. Legal & Compliance	To assess whether there is a robust Integrated Programme Plan along with a good release strategy to support the release and rollout of SPMP to branches. This will encompass: 1) Alignment of the Programme Planning with the Technology Delivery Roadmap. 2) Current status of the Programme Plan in relation to targets, timelines and budgets clearly defined. eg Backlog Management. 3) KPI's and related measures that demonstrate effectiveness of planning and how poor trends (early warnings) are addressed. 4) Review process, controls, methodology supporting planning and release. This will cover historic (eg lessons learnt) and planned (eg identified risks) to ensure effective and aligned with good practice. 5) Reporting, communication, and document controls effective. 6) Application of good practice application and management of Agile methodology. 7) Organisational clarity and defined R&R in this arena. 8) Integrated plan and milestone management/governance.	A robust integrated programme level plan exists combining the technology delivery roadmap, including clear documentation of assumptions, dependencies, and milestones. Also proving this has been tracked and regularly reported by PMO.

15	Vendor Management / 3rd Party Management	1.Security 2. Retail 3. Contract Management 4. Legal & Compliance 5. Business Support 6. Procurement	To assess and review the robustness of POL policy, process and governance applied to the selection, acceptance and controls established to obtain vendor / 3rd party support for the SPMP Programme. Review the adequacy of vendor management and performance related process and procedures. Review design and oversight mechanisms for 3rd parties.	There is clear evidence that the vendor selection process and compliance to policy has been applied and effectively managed. With the relevant up to date DOA applied to spends and approvals. Ensure robust vendor performance management and monitoring is in place.
SOW #	**Title**	**Key Pillars**	**Scope**	**Assurance outcome**
16	Software Delivery Life Cycle	1.Governance 2. Software Development 3. Security 4. Data 5. Retail 6. Business Support 7. Transaction Integrity	The review will focus on: • Performing sample reviews on key process and procedures eg JIRA, EPIC and User stories, Coding Standards, Tooling, test scripts etc. Assessing application of standards, practices and quality frameworks. • Assess whether robust policies and procedures are in place to manage 'change control, to ensure alignment with business requirements but also delivery of BC objectives and outcomes. • Review whether appropriate Governance (incl KPI/KRI) and oversight exists. • Review how PMO understand and assist in the identification of risks, issues, assumptions, and dependencies. • Assess how the Programme Team drive continuous improvement.	To ensure that good practice has been applied across Governance Gates and protects integrity of the code For environment change requests a formal and established gating process and procedure are embedded. Detailed evidence retained to ensure that the correct level of attention has been applied to ensure the desired outcomes of the SPMP platform delivery/BC. Also, identification of any potential deviations and how change management principles have been applied managed correctly.
17	Enterprise Assets Logging Enterprise Asset Software	1.Security	To perform a deep-dive technical assessment into available system logs relating to security and incident monitoring. The scope of the review will focus on: • Assessing the processes and data sources available that relate to the logging functionality for security events and sensitive transactions. e.g. Review logging functionality for security events, review the logging functionality for sensitive transactions • Review the process designed to analyse the logs and address exceptions • Review the process designed to respond to suspicious activity discovered in the logs (manual, automated), and any incident response and handling. Management of PEN's including planning, remediation and closure.	To ensure that rigorous processes and controls are in place and followed to support enterprise assets logging and software. And detailed evidence exists to demonstrate the logging functionality for security events and sensitive transactions are robust and in line with good practice and required policies. With relevant processes to support monitoring, reporting and taking preventive action.

SOW #	Title	Key Pillars	Scope	Assurance outcome
18	Network Infrastructure Network Monitoring	1. Security 2. Retail 3. Transaction Integrity	Assessment of network architecture, configuration, and security controls. Evaluation of firewall configurations, intrusion detection/prevention systems, and network segmentation. Review of network devices, such as routers, switches, and access points, for vulnerabilities and misconfigurations. Web & Email Browser Protection / Cyber Security. Assess whether good practice (eg ISO) have been applied to security architecture, vulnerabilities, monitoring for change and configuration controls. Review will also focus on the network monitoring controls to ensure countermeasures are deployed to prevent intrusions and attacks to the network. The review will also encompass: 1. Configuration management system: to track and manage configurations of network devices 2. Baseline configurations: establishing and maintaining secure baseline configurations for different types of network devices to reduce vulnerabilities 3. Change management processes: to ensure that any changes to network decide configurations are documented, reviewed, and authorised 4. Vulnerability scanning tools 5. Patch management 6. Network segmentation 7. Logging and monitoring systems 8. Incident response plan 9. Employee training 10. Regular audit and reviews.	Clear evidence of robust controls & processes, with supporting evidence / artefacts, confirming the network infrastructure and measures are managed in accordance with good practice and defined POL / Regulatory requirements.

SOW #	Title	Key Pillars	Scope	Assurance outcome
19	Application Software Security	1. Security 2. Software Delivery 3. Retail 4. Data 5. Inquiry	Review of Application Security to ensure that relevant tools have been deployed and monitoring activities are in place to prevent and detect intrusions and attacks. Assessment of application development practices, including secure coding standards and vulnerability management. Review of application architecture, design, and access controls. Penetration testing and vulnerability assessments of web applications, mobile apps, and other software systems. The review will also encompass: 1. Static Application Security testing (SAST) 2. Dynamic application security testing (DAST) 3. Security training for developers 4. Secure development frameworks 5. Incident response plan for application security 6. Dependency scanning.	Programme can demonstrate that there are robust processes and procedures in place to demonstrate practices and testing to prevent and detect security risks at an application level.
20	People & Culture	All pillars, key focus on 1 Governance 2. Legal & Compliance 3. A&CI 4. Contract Management 5. Culture 6. CIJ 7. Business Support 8. Retail 9. Inquiry	Review will focus on SPMP Roles and include validation: To assess whether the SPMP programme has adopted and embedded the appropriate process and procedures in place to embed the right culture and people into the organisation aligned with achievement of strategic and operational objectives. Assess how key cultural and people thematic from CIJ and HIJ are applied and sustained. To review the establish the effectiveness of WoW and how managed across the programme. Assess how TOM for business support and BAU Retail Operations embed the right cultural and people values aligned with the issue judgements. Review the training in place upon entering the POL and the subsequent training that supports employees understand and adhere to the culture aspects of POL. Assess how new roles and specs are created to ensure alignment with business purpose and objectives. Set KPI's / measures in place to identify success in this area (eg attrition) and how poor trends are addressed.	Clear evidence available demonstrating good practice covering all elements of people and culture across the programme. This will include: 1) Records of training covering onboarding new staff and ongoing training supporting identified training needs 2) Effective comms to support staff and advise of current / new initiatives in this area of the business 3) Measures of effectiveness of WoW culture 4) How lessons learnt have been addressed 5) KPI's / Measures in place to identify poor trends (eg attrition) and how they are resolved / mitigated 6) Clear reporting to the senior team on status, risks, issue resolution and planning.

SOW #	Title	Key Pillars	Scope	Assurance outcome
21	Incident Response and Management - Penetration Testing	1. Software Delivery 2. Security 3. Retail 4. Legal & Compliance 5. Data 6. Inquiry	To ensure that Penetration Testing is fully controlled in alignment with good (business / Regulatory / ISO) practice. Scope of this review will also look at: • intelligence gathering eg network and domain names, mails server to see how targets are focussed and vulnerabilities identified. • Process and controls around incident management including but not limited to: • Incident response plans, procedures, and capabilities. • Backup and recovery processes, including testing and validation. • Incident detection and response tools, processes, and training.	To have obtained details of established processes and controls around the E2E penetration testing activity.
22	Business & IT Controls Library	1.Governance 2. Software Delivery	Assess Business Controls/IT that have been documented to date for programme/POL. Assess how control coverage and design is adequate and covers the risk landscape of SPMP/POL. Assess the applications of these controls and identify and gaps of application/remediation. Scope of this review will also look at • Risk library (business and IT) • Control library (business and IT) • RACI by process and controls • DOA • SoD and Access Management • Security and Integrity • MI/Reporting and Governance, including REN and PENs.	POL is able to monitor and measure the efficacy of it control environment vs the release profile of SPMP.

SOW #	Title	Key Pillars	Scope	Assurance outcome
23	Governance	All Pillars	Review the Governance arrangements within SPMP to ensure robust practices exist for: • Progress Tracking and Reporting – tracking and reporting of progress including the programme financials is in place on the programme; status reporting takes place to ensure that progress is being tracked and reported on the programme. Tracking, monitoring SPMP progress • Monitoring of KRI/EWI • Sufficient objectivity is in place to constructively challenge SPMP direction, risk assessments and outcomes. • Change management process and practices • Monitoring of BC and delivery of BR • Oversight of issue judgements • PM protection • Efficacy of reporting data sets with key business and SME input • Decision making and risk assessments • Planning and Dependency Management • Programme Structures - a RACI matrix is defined and in place for the programme and roles, responsibilities and accountabilities have been clearly defined and key roles on the programme have been filled. • Communications and Stakeholder Management – stakeholder mapping and communications plan for the programme is defined; lower-level communications plans outlining the timing of activities and responsible individuals has been defined for the programme. • Resource Management – there is a resource plan defined for the programme; ensure that the plan is maintained, and regularly reviewed and updated • Risk acceptances, inputs and continuous monitoring.	A robust governance approach in place to ensure successful delivery of SPMP in line with BC and BR.
24	Integration strategy (To POL strategies and wider systems)	1. Software Delivery 2. Data 3. Legal & regulatory 4. Contract Management	Review approach to systems integrated with the new NBIT platform to ensure they are/will be integrated and transferring, providing information accurately and timely between different systems. Review and understand what MI/reports and KPI's are in place to manage and monitor transference of data between systems, to ensure completeness, accuracy, and timeliness of transfer. Review whether sufficient and relevant integration testing has been carried out and signed off as part of the stage gating process by relevant and authorised individuals.	Evidence of a robust integration Strategy with other systems (SWIFT, Banking apps) Master data being relied upon by the programme is accurate and there are no inaccuracies in product set up or mapping. Ie no risk that results in incorrect postings to downstream systems. Systems integrated with the SPMP platform are providing accurate information and supporting evidence (controls/measures) are in place Accurate MI/KPI/Reporting available and evidence of effective action taken to address issues/poor trends. Evidence of testing conducted and completed with supporting processes and best practices controls Evidence to demonstrate that the key stakeholders have been engaged as part of the sign off / gating process.

SOW #	Title	Key Pillars	Scope	Assurance outcome
25	Legal Risk	1. Security 2. Legal & Regulatory	Review the Legal Risk Framework to evaluate and assess how: 1) Sources of legal risk are identified, e.g. contracts, regulatory, structural changes, and compliance. 2) Risks are defined vis a vis risks vs issues vs potential risks and potential issues. 3) Risks processes and controls to ensure risks are appropriately identified, managed and monitored. 4) RACI and DoA for management and assessment of Legal risk is appropriate and understood. 4) Monitoring and KPI - Aligned with high and low risk legal issues with appropriate planning to support. 5) Defined controls and measures aligned with HIJ / CIJ, and lessons learnt. 6) Alignment is assured with Programme Deliverables and Gating / No Go decision making.	Clearly defined processes with supporting evidence to demonstrate the controls and management of legal risks.
26	Retail Readiness and Support to Post Masters	Retail Business Support / Hypercare	The purpose of the review is to ensure the SPMP programme can demonstrate robust processes and procedures, which validate the retail readiness to receive the new platform from a Postmaster lens (PM). • Retail PM readiness plans – coverage and conformance with principles laid out within issue judgements. • PM Support and Training. • PM comms/engagement plans. • BSC Readiness – detailed procedure manuals etc. • Hypercare Arrangements. • PM Hardware and Commissioning. • Communication to PM's – clarity, approach and impact. • Role of BA and AM / RACI. • Transferring and cut off procedures from Horizon to SPMP. • PM routes to escalation and POL resolution SLA, and approach. • Approach and role of A&CI and Retail Assurance teams. • Plans for resourcing to ensure delivery. • Governance, KPI and Risk Management. • Adequacy and effectiveness of early warning indicators, with a key focus on PM wellbeing (CIJ). • Culture -Has PoL/Retail identified the right and appropriate mechanism and triggers to capture culture.	To have ensured that all elements of the Retail Readiness process is effectively Managed and providing the best level of control and support to Post Masters as part of the programme delivery requirements. Evidence obtained to demonstrate planning accuracy, efficiency in stock control, delivery planning, product verification, KPI's monitored to ensure poor trends/performance addressed, swap out and post-delivery support. Evidence of financial controls/planning and alignment with the Programme Plan will also have been validated.

SOW #	Title	Key Pillars	Scope	Assurance outcome
27	Cloud Security	Security	• Assessment of cloud infrastructure configurations (e.g., AWS, Azure, GCP). • Review of cloud service provider (CSP) security controls and shared responsibility models. • Evaluation of cloud identity and access management, data encryption, and compliance posture.	Ensured that controls, processes, and measures managing the cloud infrastructure, CSP security controls and identity and access management are in place and align with good business practice Ie ISO 27001.
28	End Point Security	Security	• Assessment of endpoint protection solutions (e.g., antivirus, endpoint detection and response). • Review of endpoint configuration management and patch management practices. • Evaluation of mobile device management (MDM) and bring-your-own-device (BYOD) policies.	Ensured that robust controls, processes, and effective measures are in place to manage endpoint protection, configuration, patch management and mobile device management. ISO 27001 / 27002.
29	Compliance & Regulatory Requirements / Frameworks	Security	• Assessment of IT controls against relevant regulatory requirements and industry standards (e.g., ISO 27001, NIST Cybersecurity Framework). • Review of compliance with specific regulations (e.g., PCI DSS, HIPAA, GDPR).	Validated, with supporting evidence, that all the programme IT controls are in compliance with POL and regulatory requirements. (e.g., PCI DSS, HIPAA, GDPR). The application and management of this being aligned to good business practice Ie ISO 27001.
30	Security Risk Management *Potential to merge with SOW 24	Security	• Evaluation of risk assessment methodologies and risk management processes. • Review of risk treatment plans and mitigation strategies. • Assessment of risk monitoring and reporting mechanisms.	Ensured the E2E Risk Management process is robust and followed in line with defined controls & processes. Evidence / artefacts seen to confirm good practice supporting risk assessment methodology, risk treatment / mitigation and effective monitoring. Good industry practice being aligned with ISO27001.
31	Security Operations (Organisation)	Security	The scope of Security Operations will be to look at the designed or to be designed Security Organisation (TOM) and assess: • Evaluation of security operations centre (SOC) processes and capabilities. • Review of security monitoring and incident detection tools. • Assessment of security incident response workflows and procedures.	Ensured that robust and defined Organisational Design including controls and processes are in place and followed to manage the security operations centre. Validated, with supporting evidence, the effectiveness of security monitoring / incident detection and response controls. This all being aligned with POL, regulatory requirements and good business practice Ie ISO 27001.
32	Disaster Recovery and Business Continuity	All Pillars	Review to ensure that POL standards are adhered to for Disaster Recovery and Business Continuity. Review to include assessment of: • measures of effectiveness and how controls are tested and enhanced to align with pre and post (Final Platform) deliverables. • DR and BC RACI. • Approach to integrated testing, including approach to cyber threats • Roll back process and procedures	To ensure robust DR and Business Continuity plan is in place with supporting processes. Detailed evidence of how the plans are tested to ensure effectiveness and alignment with the platform during release phases and current planning(preparation) for final release. Full ownership and RACI to support this model has been defined. All planning aligned with good business practice and POL / Regulatory requirements

SOW #	Title	Key Pillars	Scope	Assurance outcome
33	Finance & Cost Model	1. Governance 2. Finance 3. Inquiry	To review the Financial Cost modelling of the SPMP programme to ensure that costs being incurred are accounted for are completely and accurate. Including the accounting principles being followed. Review the linkage of the cost model to the Business Case and Business Requirements. And how changes in the Business Case and Business Requirements are being reflected into the Finance Cost Model. Review the processes in place to monitor and manage Actuals to Budget/Forecast. How exceptions and deviations are being escalated and addressed.	Ensure that there are robust processes and procedures in place to capture and appropriately account for SPMP cost, including the monitoring and reporting against budgets /forecast. Ensure alignment with BC and BR.
34	Business Case and Benefit Realisation Assurance	1.Governance	The scope of the Business Case and Benefit Realisation review will consider: a Modelling for business case and benefit realisation is sufficiently robust and appropriate b Sufficient to support funding draw downs c Captures impacts of risks, issues and assurance reviews/outcomes d BC and BR change management process is robust.	Ensure that there is a robust model in place for the Business Case and the linkage into Business Requirements and delivery. Provide an opinion on the Cost, Benefits realisation model and assumptions. Provide opinion on the monitoring and reporting mechanisms of the Business Case and change management.